

EPA
Electronic Reporting for NPDES Permittees
Proposed Rule
Review & Comments

Draft

31 December, 1998

Introduction

The EPA is preparing to release a draft rule that will support the first opportunity for wide use of X12 EDI for a major compliance report — the discharge monitoring report (DMR). ~~Paper DMRs replicating that certification.~~

There is substantial Federal policy and legislation committing federal agencies to electronic commerce (EC). However, there is not any policies as to how agencies should adopt or conduct EC or what technologies they should use beyond FIPS 161-2. There is even less policy on how to employ or process digital signatures of either government official or private industry representatives. Currently different agencies are exploring a variety of technologies for applying digital signatures including: biometrics, token cards, and PKE/PKI, however, none has emerged to be the definitive choice for federal wide use. ~~At least within the environmental enforcement sectors of the EPA and DoJ~~ there remain concerns about enforceability of digital signatures and maintaining electronic records especially for use in criminal prosecutions.

The current draft [EPA NPDES EDI rule (EPA 40 CFR Parts 122 and 123 - Establishment of Electronic Reporting for NPDES Permittees, dated 10/1/98)], addresses the use of a combination of an electronic PIN number (that is unique to an individual), and a certification statement (a.k.a. "follow-up postcard") that corresponds to the electronic DMR and which bears the individual's hand-written signature and authenticates the accuracy of the data submitted electronically. While not optimal, as it continues use of paper and may lack a clearly provable link between the "post card" and the EDMR data, the approach has been reviewed and agreed to between the EPA and DoJ

The EPA has tasked the Logistics Management Institute (LMI) to review other possibilities that the EPA can consider as addendums to the draft rule or to maintain as options in response to comments and questions made on the draft rule.

Due to EPA's requirement to quickly establish this rule¹ and a production EDI process, any alternatives addressed herein reflect an approach that can:

- Be implemented quickly
- Be implemented with minimum technology and cost to both the EPA and the DMR user community
- Satisfy the minimum requirements to address EPA/DOJ concerns ~~for data integrity which includes a handwritten signature on paper~~
- If possible, be used as a stepping stone to a longer-term solution, thus leading the DMR user

¹ This document does not attempt to review the text in the draft rule, but rather, specifically addresses short-term certification and assumes that the reader is familiar with the draft rule

community through a process that can be applied to future implementations, allowing their comfort level to grow with their experience of each phase of the implementation

Overview

The intention of this "PIN & Postcard" system, is to allow EDI submissions to take place, thus expediting the process for both industry and government, while still maintaining minimum EPA/DOJ requirements a high standard of proof that would apply in a criminal proceeding based on the falsification of a DMR submitted electronically. Hence the EPA and DOJ are still requiring a paper based handwritten signature to be associated with the EDMR (until such time as acceptable federal guidelines for electronic signatures are developed).

The draft rule requires the submission of a paper "postcard" to be submitted with each EDMR. The "postcard" will contain the following basic elements:

1. Permit identification and transmission ID number
2. DMR monitoring period
3. Identification of each outfall reported on the EDMR
4. Certification/signature

Additionally the EDMR will carry a PIN assigned by the EPA which must correspond to the individual signing the "postcard."

The following pages contain brief reviews of this post card approach and several alternative options and provide some pros and cons for each. We must state, however, from the outset that as long as a handwritten signature is required along with an electronic record, we do not believe there is a solution that: reduces burden, can be widely deployed and convenient to use, and meets ~~DoJ security~~ security concerns. All of the approaches except the last one, follow the constraint of requiring a hand-written signature. The last offers one solution for an electronic only solution, for purposes of comparison.

Assumptions

As these options were considered certain assumptions were made about the user community that would submit EDI DMRS:

- That submitter already has or will develop a data base of discharge monitoring data. The submitter would then develop additional programs to automatically extract the data, convert it into an X12 EDI transaction set, and transmit it to the EPA.²

² The reader should note that the EDI format is itself not easily readable and that the typically two-three steps required to extract and convert the data present opportunities for mistakes to be made, and for someone to claim that

- The number of participants will be small in the beginning

Key Issues

Throughout most of the options to be discussed a few key issues will recur:

- *Ensuring a valid electronic signature* — The first requirement is to ensure that some form of digital mark has been applied to the document and that it is a valid one for an EPA recognized individual associated with that facility and submission.
- *Linking the signature to the electronic transaction* — In a totally electronic environment the second requirement is to ensure that the data was not manipulated after the digital signature was affixed. In the envisioned DMR process the requirement will be to *clearly link the handwritten signature to the electronic data and to ensure that the data was not manipulated after the signature*.
- *Cost and availability* — Paper copies are filed and while there is an expense associated with this it is not high. Further the document which contains both the data and the certification can be pulled from the file at need and stand on its own. Dealing with electronic records that might someday be legal evidence will require maintaining a perfect copy of the electronic document with assurances that it not been tampered with, and maintaining a “chain of custody” of how it was dealt with. To do this, the EPA will have to deploy hardware, software, policies and procedures to preserve and protect the electronic record. This will be a substantial increase in burden – not decrease. To an extent the submitting facility may also see an increase in burden to process both paper and electronic media.

Option 1 – No electronic reporting

Description:

No electronic reporting of DMR data.

Pros:

- Relieves the EPA and industry from dealing with the issues involved with non-repudiation of electronic reporting.
- Allows the process to continue the way it has in the past, so there is no learning curve or additional investment in technology required for either government or industry.
- Alleviates the concerns of the EPA and the DOJ related to criminal prosecution based on electronic reporting procedures.

Cons:

- This approach is listed purely for the sake of completeness and to identify that it neither progress nor acceptable and that therefore some one of the following solutions (or some other) must be found to be acceptable by all parties.
- Does not support either the President's or the EPA's goals for electronic reporting, i.e.:
 1. The President's "Reinventing Environmental Information Report", March 1996.
 2. EPA "Notice of Agency's General Policy for Accepting Filing of Environmental Reports via Electronic Data Interchange (EDI)", 61 FR 46684, September 4, 1996.
- It does not help to reduce the amount of paperwork that is required to report.
- Does not expedite the reporting process. Requires advance planning to complete the hardcopy DMR form, as well as time and extra cost to ship via USPS, overnight express, etc.

Option 2 – X12 Submission & Postcard

Description:

This is the postcard as it is described in the draft rule, and would contain the following:

1. Permit identification and unique transmission ID number
2. DMR monitoring period
3. Identification of outfalls
4. Certification

Pros:

- Already approved by EPA and DOJ for use
- Has undergone the scrutiny of the EPA and DOJ and has been determined to meet the high standard of proof required in a criminal proceeding
- While still requiring a paper submission it reduces in size and content what is submitted in a traditional DMR
- It implies multiple levels of linkage and identification through the transmission number, the pin, and the cer

Cons:

- The postcard contains the outfall numbers, BUT NOT THE ASSOCIATED PARAMETER READINGS. The lack of the parameters may make it difficult to prove the linkage between the individual and any claim by EPA/DOJ that the individual knowingly misrepresented the parameter values received by the EPA in the EDMR. Since the PIN number and/or password are not referenced on the postcard, the link between the electronic submission and the postcard is not strong. If either the PIN or the password (or both) were referenced on the postcard, there would be less potential for dispute later that the two were somehow linked. Doing so however, would be at the risk of the security of the PIN and/or password as they are used in the electronic submission, and is not recommended.
- It can also be argued, that the PIN number on the electronic submission can be easily compromised, if it is not encrypted in any way when used. Likewise, since transmissions are done electronically, this PIN is part of the electronic transmission, and as such, is stored in various computer systems in plain text. A responsible authority could easily argue that their computer operator viewed an archived transaction and sent an unauthorized transaction on their behalf. So, the PIN number alone does not constitute a non-reputable transmission.
- The approach does not eliminate the submitter from claiming that the government either deliberately or inadvertently altered the EDMR after receipt. There may be no way to reliably link the two pieces of evidence together. The above scenario could be used by a submitter to falsify data, and then argue later that the data was somehow modified - either by one of the computer systems involved in the transaction, by the

government, or by some third party.

- The post card minimally reduces burden on the submitter. It would be expected that the submitter will print the postcard data from his database and then sign and mail it. Otherwise preparing both the “post card” and the 863 by “hand” represents a significant burden increase.

Option 3 – X12 Submission & fully printed DMR.

Description:

1. The submitter creates an electronic DMR and transmits it to the EPA.
2. Prints a copy of it in paper DMR format – with ALL DMR data being present.
3. Signs the DMR and mails it to the EPA.

Pros:

- Much easier to prosecute cases based on full hard-copy version being signed.
- Eliminates the extra burden upon the EPA to establish policy, procedures, hardware, software, and staff to preserve “archival” copies of the received data for legal purposes.
- Allows the process to be expedited for the EPA, as the electronic submission can still take place. The follow-up is via this hard copy.

Cons:

- Full DMR may be much larger than the postcard. However, since the computer is printing it the difference in time and expense may be negligible.
- Like the post-card, this option loses much of the benefit of electronic reporting, since both paper and electronic copies must be processed and at least periodically the two must be checked against each other.
- As the facility continues to submit the full DMR it creates the perception of a lack of progress and of additional work.

Option 4 – X12 Submission & Echo Back

Description:

1. The submitter initially transmits only the 863 with PIN
2. The EPA receives the 863 and converts it into a readable format and sends an “echo back” copy back to the submitter. The returned copy could be either before or after PCS processing of the data and may consist of only the “raw” data or PCS status (e.g., contains errors, is or is not within compliance boundaries).
3. The submitter would sign the document which could either be the full copy, or the post-card, or some other variant on the two and mail it back to the EPA.

Pros:

- As the EPA prints the material (post-card or full DMR) and mails it back to the facility, it creates the perception of reducing the burden upon the facility.
- The facility reviews the data as received at the EPA, reducing concerns that the EPA received it incorrectly or tampered with it.

Cons:

- Time would have to be built into the process for the submitter to validate the echo backed file and generate the postcard, and then for the postcard to travel through the mail.
- Requires the facility to re-validate the EPA echoback copy against their original submission.
- Loses much of the benefit of doing the transaction electronically, since the process now becomes more instead of less complex. From the submitters perspective this adds burden without lessening the existing burden, and little is gained.

Option 5 – Use of Scanners and PDF

Description:

This option can be used with any of the other options. Rather than mailing the hard copy. The submitter can sign the post-card, the full DMR or any other document and scan it into a PDF format and e-mail it.

Pros:

- Eliminates managing the paper copy and allows the certification document to be “bundled” with the X12 data for archiving.
- Eliminates the delays associated with the mail and the requirement to process paper, and to link the paper copy to the electronic file.
- In the most technically sophisticated version the PDF file could be transmitted in or with the EDMR.

Cons:

- Has all the negatives associated with the option the scanner supports plus the requirement for the facility to obtain scanner hardware and software and deploy it.

Option 6 – X12 Submission & Postcard (with secure hash reference)

Description:

This is a modified version of the postcard that would contain the following:

1. Permit identification and unique transmission ID number
2. DMR monitoring period
3. *40 character (160 bit) SHA-1 hash of the data*³
4. Certification

The government would electronically 'echo back' data to each submitter, probably via electronic mail. This data will be comprised of two basic pieces, each likely an email attachment:

1. Data file for verification

An electronic copy of the submitted data, in whatever format is deemed most usable (i.e.: PDF, ASCII, MS Word, etc.). The submitter will use this to verify the integrity of their electronic submission and to use as a basis for the secure hash.

2. Printable postcard file

A pre-filled out electronic version of the postcard as described above, in whatever format is deemed most usable (MS word, PDF, etc). This postcard would contain a Secure Hash Algorithm 1 (SHA-1) hash of the data attachment pre-filled out on the form, as well as all the other elements required. It would be a complete printable copy of the postcard that the submitter could print, sign, photocopy, and mail.

The submitter would:

1. Verify the contents of the data file, by either electronically comparing it's contents to their own original submission, or doing so manually.
2. Confirm the SHA-1 hash provided in the postcard file, by running their own SHA-1 software against the provided data file.
3. Having done both of the above, the submitter would print the postcard, sign it, make a photocopy for their files, and mail the original to the government.
4. The submitter would also archive the following:

³ Note: Hash coding is applying a mathematical formula to the characters of the data file to compute a unique number. Any revision of the text will cause the resulting number to no longer match the original number. This verifies that the data has not been altered. While use of hash coding has been presented as a single option, it can like the use of

- Electronic copy of the email, including the attachments
- Electronic copy of the software used to generate the SHA-1 hash (so that it can be reliably reproduced if necessary)
- Photocopy of the signed postcard

Pros:

- The postcard truly becomes a postcard, since the requirement for the amount of information on the document is drastically reduced.
- The electronic submission allows the process to be expedited, while still allowing for a reliably signed official copy, without excessive burden on behalf of either the government or the submitter.
- Both parties (the government and the submitter) are assured that what is being signed for is an accurate representation of the actual data that they both possess. SHA-1 is the government standard (FIPS PUB 180-1) for producing a reliable one-way hash. It is also the most trustworthy, based on current technology. The SHA-1 process, while mathematical in nature, is common enough of a general approach, that it should be relatively easy to explain in a courtroom. The fact that it is the government standard, makes the procedure easier to justify.
- Both parties (the government and the submitter) have proof that will stand up in court, as the combination of the unique transmission number, SHA-1 hash value, and the submitter's signature will certify that the submitter agrees with the DMR information as EPA has represented it back to them. This will provide a stronger link from the postcard to the transmission than is currently available in the proposed rule.
- The process of obtaining and utilizing SHA-1 software is simple enough that there should not be a complaint regarding complexity. There are both freely available and commercial sources for SHA-1 software. Having options gives both the government and industry the ability to use whatever works best for them. The cost of entry is low for everyone involved. There are SHA-1 COTS options that run on a variety of platforms (including the popular Microsoft Windows varieties), and cost less than one hundred dollars.
- Since SHA-1 software is commercially available from a variety of sources, issues that could have arisen if the government provided the software will not be a concern. This should add to the trustworthy factor. The government can still make non-commercial versions of the software freely available to industry for convenience and/or testing, in order to expedite the process. Industry can choose whether or not it desires to use government developed or referenced versions, purchase COTS software, or develop their own version based on the government standards (which are widely available). Note: a list of validated SHA-1 products is available from the National Institute of Standards and Technology (NIST).
- Since it is both the government standard and the most reliable method currently available, a SHA-1 hash will very likely be part of a more complete electronic reporting solution in the future. Taking this first step now will allow both industry and government to start getting familiar with technology that will be part of the future process. This will be a good test of the process, as well as a good indication of industries ability and willingness to make this happen. Likewise, it will allow the government to step into the legal issues in the same manner. There is a natural progression from a simple hash to the implementation of a full electronic reporting process.

Cons:

- There is still much more data to verify, since the entire 863 is duplicated, although in electronic form. If done properly, and in cooperation with industry, the electronic echo back of the 863 data could be provided in a format the industry could electronically verify, saving them the time and expense of doing so manually. This would likely make the data file less readable by humans, but much easier to validate.
- The SHA-1 software will need to be obtained and installed by each company that is going to be involved. The government can help by providing a list of sources for the software, as well as providing documentation describing the technology, basic installation, and usage, etc.
- The government (EPA) will have to review available SHA-1 software options (government, publicly available and commercial) and put a process in place which utilizes the technology for their own internal use.
- The government's legal representatives (EPA/DOJ) will have to review the technology, to determine if it's use is a viable alternative to the current postcard design. While this is not necessarily a negative point, this will take some amount of time. Having this process available to industry in an expeditious manner is a high priority, so this must be considered.
- Time would have to be built into the process for the submitter to validate the echo backed file and generate the postcard, and then for the postcard to travel through the mail.

Option 7 – X12 Submission via Trusted Third Party

Description:

This is option would have the EPA contract with a commercial third party, most likely a commercial EDI value added network (VAN) to act as a trusted third party. Key to this approach is that the facility would transmit the EDMR to the VAN and the VAN would forward it to the EPA. Both the EPA and the facility would sign an initial trading partner agreement binding them to the electronic copy of what the VAN retains.

This approach could be used in conjunction with any other, that is the post card or the full DMR could also be paper signed and forwarded to the VAN for retention.

Pros:

- Especially if used only with the EDMR streamlines the process for both the EPA and the facility.
- Eliminates the burden upon the EPA, PCS process with managing the archival/legal aspects of the EDMR.

Cons:

- This option would likely be very expensive. The EPA would have to contract with a VAN to provide these services which are beyond the range of normal VAN services.
- Continues to leave open that the electronic record becomes altered (deliberately or accidentally) during or after transmission.
- There may be fears on the part of both the facility and the EPA that the VAN would be biased on a part of the other side and might alter the records.
- Would the prior agreement be sufficient in court.

Option 8 Using a Digital Signatures.and PDF

Description:

This description varies significantly from the previous ones, in that it uses only an electronic digital signature. Further, this option uses a web-form to submit the data rather than the EDI 863. In addition to this approach there are other electronic “signature” technologies that can be used either with X12 EDI or web forms. These mostly include appending some form of secure password using public/private key combinations, personal physical tokens (smart cards); biometric techniques, and others as well. These can also be used in combination with hash coding (previously described) or other encryption techniques to protect the overall contents of the document.

Adobe Acrobat 4.0 (now in beta) scheduled for release Spring 1999 allows digital signatures to be used as a form field in PDF documents. In addition to capturing form data, the PDF form now has the capability to capture and verify multiple signatures. In addition, the functionality exists to verify integrity of the data through hash algorithms. Changes can be detected and identified by “rolling back” to previous versions.

In this scenario EPA would create a PDF form version of the DMR with a digital signature block. The submitter would download this form off of the EPA web site and then use their copy of Adobe Exchange 4.0 (as part of the Acrobat suite) to complete the form. The submitter would then sign the form with their digital signature certificate. This certificate could be provided by any number of third party certificate providers who are supporting Acrobat 4.0, including PKI vendors Entrust and Verisign, biometric signature providers such as (digisign?), and the native Adobe Self-Sign signature handler provided with the product. After signing, the form cannot be changed without having to resign the form, and changes can be detected with a hash algorithm. Changes can also be viewed by “rolling back” to previous versions in the signature chain and comparing versions. The signatures can be validated on-line against revocation lists anytime the document is opened. After completing the form, the submitter could e-mail the file to EPA or send the file using regular mail. At EPA the form would be opened, the signatures validated, and the data exported to the database.

Pros:

- Allows form data to be captured and stored with signature.
- No paper follow-on signature.
- Changes can be detected and identified through secure hash algorithm.
- Form data can be exported into database.
- Supports client-side data validation checks that can improve data quality.
- Does not require any programming or database download on part of submitter.
- Supports biometric signatures
- Digital signature handlers provided by numerous third-parties.
- Most applicable to numerous smaller users without their own discharge monitoring databases. EDI would be more beneficial to larger reporters with data bases.

Cons:

- DoJ may not yet be willing to accept a totally electronic approach
- Proprietary, not standards-based solution (although security standards such as X.509 are adhered to). Submitters must purchase Adobe Acrobat 4.0 software (estimated price - \$295).
- Not Web-enabled yet – data is transferred through e-mail or file transfers (although form/Java scripts can be down-loaded to users machine via a browser).
- A process must be developed for registering certificates and digital ID's.
- Harvesting data generally requires opening up file and then exporting data to flat file.

Considerations for the Future

In order for electronic DRMs (or any compliance report) to be conducted with reduced burden (for both the external user and the EPA) *the paper must be eliminated*. The question then becomes determining the most appropriate technology to use to apply a digital signature. Optimally this technology will be:

- Both secure and simple enough to ~~obtain DOJ support and be successful in court~~
- Part of or compatible with a Federal standard for digital signatures
- For external users
 - ◆ Widely available
 - ◆ Inexpensive to obtain
 - ◆ Easy to use

Additional bullet: “A system they feel confident in using.” (Or something to the effect that in addition to maintaining federal enforceability the external users almost must be confident that the system is reliable and protects their submissions.)

- National standards based that is non-proprietary

Aren't all the scenarios somewhat proprietary, except for the postcard and SHA approach? Even the hash approach might turn out to be somewhat proprietary if EPA must require submitters to use products that have gone through some sort of validation.

Various effective technologies exist for employing a digital signature, but none has achieved *sufficient recognition* or been adopted across a *sufficient base of use* to meet most of the above criteria. The EPA must continue to explore the most effective technologies for its community and be proactive in working with DoJ, other agencies (federal and state) and federal cross-agency security organizations to establish a coherent Federal approach.

Anything short of electronic (only) submissions will serve only to add to burden, create frustration on the part of the users, and likely draw criticism from organizations such as OMB.

While exploring and resolving the issue of electronic signature the EPA should be developing it preferred architecture and procedures for web and EDI based compliance reporting and developing procedures for other aspects of security including archiving, maintaining facility and user identifications, etc.

Conclusions

As previously stated, we do not believe there is an optimal solution for this problem at this time given the constraints. Of those options that possess a paper signature we recommend Option 3 - printing the full DMR. We recognize this solution does not appear to represent any progress at all. However, it is a database to database via EDI solution, It GUARANTEES legal accountability, and is less inconvenient than it may appear as the database can easily print a DMR equivalent form, and it minimizes the electronic security requirements to be implemented by the EPA. No other solution does this.

Given the difficulties involved it may seem that it might be prudent to delay implementation until clearer Federal policy emerges or technology improves. However, we believe that the EPA must actively pursue electronic reporting to meet both federal and EPA goals for paperless government. Further, unless these issues are raised and have practical impacts they will continue to be unresolved.

must eventually be supported through both X12 EDI and the world wide web.